The GDPR Transfer Regime and Modern Technologies

Tudorica, Melania; Mulder, Trix

Published in:
Proceedings of ITU Kaldeioscope

Publication date:
2019

THE GDPR TRANSFER REGIME AND MODERN TECHNOLOGIES

Melania Tudorica; Trix Mulder

Rijksuniversiteit Groningen, the Netherlands

ABSTRACT

Health data comes within a person's most intimate sphere [1]. It is therefore considered to be sensitive data due to the great impact it could have on a person's life if this data were freely available. Unauthorized disclosure may lead to various forms of discrimination and violation of fundamental rights. Rapid modern technological developments bring enormous benefits to society. However, with this digitization, large amounts of health data are generated. This makes our health data vulnerable, especially when transferred across borders. The new EU General Data Protection Regulation (GDPR) legal framework provides for rights for users of modern technologies (data subjects) and obligations for companies (controllers and processors) with regard to the processing of personal data. Chapter V of the GDPR protects personal data that are transferred to third countries, outside the EU. The term 'transfer' itself, however, is not defined by the GDPR. This paper examines whether transfer within the meaning of the GDPR applies to health data processed by modern technologies and if the complexity of the GDPR legal framework as such sufficiently reflects reality and protects health data that moves across borders, in particular to jurisdictions outside the EU.

Keywords – Data protection, health data, transfer, transit

1. INTRODUCTION[1]

In our rapidly evolving digital world, people use various modern technologies to track and measure their health and fitness. Modern technologies such as mobile applications and wearables (including watches, bracelets and smart fashion) are used to get into shape, keep fit, lose weight, reduce stress, manage mental health disorders, test and diagnose for specific diseases such as malaria, help with family planning and ovulation tracking, etc. The technologies enable people to monitor their own health and fitness by entering personal health data and using (pressure) sensing technologies which measure vital signs (such as heartrate) and track progress (such as counting steps) [2]. New health technologies are a key area of 21st century knowledge societies and economies, offering potential for growth and economic development [3]. It is one of the largest growing global markets. According to a recent article, there are more than 300 000 health related mobile device applications [4]. While the use of these technologies may bring benefits to society as they reduce the burden on doctors and empower people by putting them in control of their own health, in particular in low income and difficult to reach areas, the downside is that these technologies generate massive amounts of health data. Considering that health data comes within a person's most intimate sphere, it could have a great impact on a person's life if this data was freely available. Risks include discrimination and violation of fundamental rights.

There have been many reports over the past couple of years or so of data breaches and companies (routinely) sharing data. The 2018 Strava and Polar incidents immediately come to mind, but also Ovia (a pregnancy tracking app) sharing intimate information with employers and insurers [6], Facebook having access to sensitive information [7] and many more examples of health data being compromised by the use of modern technologies [8]. Our health data is particularly vulnerable if it is processed outside the protected sphere of a medical environment where health data is processed by professionals who are under the obligation of medical confidentiality. The health data that is processed by these modern technologies is, most of the time, processed by commercial companies who are generally unclear about their processing activities and with whom they share the collected data [9].

Legally a lot can be said about modern technologies, their use, privacy risks, infringements of rights, etc. This paper focusses specifically on transfer and modern technologies. Inherent to the nature of these technologies is that data is not bound by borders. Users of modern technologies may be located anywhere in the world and data may move across the globe while being processed by companies established anywhere in the world. One of the main challenges of the borderless nature of data processing is that it is difficult to track the data and as a consequence difficult to determine jurisdiction, which may lead to difficulties in data subjects exercising rights in cases of infringements.

Within the European Union (EU) data is protected by the General Data Protection Regulation (GDPR) [10]. The GDPR protects data, among other things, when it is transferred across borders. This research aims to answer how the GDPR transfer regime applies to data processing

[1] Paper accepted for presentation at "ICT for Health: Networks, standards and innovation" ITU Kaleidoscope academic conference, Atlanta, Georgia, USA, 4-6 December 2019, http://itu.int/go/K-2019.

by modern technologies, if at all, and whether the GDPR legal framework as such offers sufficient protection. When using modern technologies, the data is collected by a device (such as a smartphone or wearable) by using applications developed by commercial companies. The applications 'send' the data to the servers of the company which owns the app and which then processes the data. What exactly happens technically behind the scenes is unclear. It is therefore unclear whether 'sending' data between the device and the server of a company can be seen as a transfer within the meaning of the GDPR and whether the GDPR transfer regime applies to processing by modern technologies.

This research argues that the complexity of the GDPR legal framework does not offer sufficient protection against processing by modern technologies. By taking a technical, behind the scenes perspective and looking at whether the (technical) process of 'sending' data from a user's device to the server of a company can be seen as a transfer within the meaning of the GDPR, we argue that this process is a mere transit of data where the device functions only as a tool for the companies to collect data [11]. In coming to this conclusion, this article first needs to establish what the legal basis for processing health data by modern technologies is. We then look at the technical process used by modern technologies and whether the GDPR transfer regime applies to this process in order to conclude whether the legal basis and the GDPR legal framework offer sufficient protection to processing by modern technologies.

2. LEGAL BASIS FOR PROCESSING HEALTH DATA BY MODERN TECHNOLOGIES

The GDPR provides rules for the protection of personal data and free movement of such data in order to protect the fundamental rights and freedoms of persons. It applies to the processing of personal data of data subjects who are in the EU, regardless of where the controller or processor are established [12]. This means that the GDPR applies to any company around the globe processing data of data subjects who are in the EU if the processing activities relate to offering goods or services to data subjects or monitoring the behavior of data subjects. As such, the GDPR aims at offering a similar level of protection for EU citizens regardless of where the data is being processed [13]. This is particularly important when health data is being processed by commercial companies who are not under any obligation of professional secrecy. In previous research we have established that many companies deny or at least do not mention the fact that they process health data while in fact they are [14].

While we use the more overarching term *health data*, Article 4 (15) of the General Data Protection Regulation (GDPR) refers to it as 'data concerning health' and defines it as:

Personal data related to the physical or mental health of a natural person, including the provision of healthcare services which reveal information about health status [15].

This is a very broad definition: any information which can reveal something about a person's (mental) health is considered to be health data. In the annex to its letter to the European Commission, the Article 29 Working Party (now the European Data Protection Board [16]) clarified the scope of the definition of data concerning health in relation to lifestyle and wellbeing apps and provides criteria to determine when data processed by such apps and devices is health data [17]. According to the Article 29 Working Party, personal data is health data when (1) the data is clearly medical data, (2) the data is raw sensor data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person or (3) conclusions are drawn about a person's health status or health risk [18]. This means that, in general, data is health data when it is used or can be used to draw conclusions about a person's health. However, the Article 29 Working Party also acknowledges that in some cases the raw data itself is considered to be health data. It also acknowledges that presumably simple facts about individuals, such as IQ, wearing glasses or lenses, smoking and drinking habits, membership of patient support groups, etc. are considered to be health data. In our view, the mere fact that a person uses an app, for example to help quit smoking or to count calories already says a lot about a person. Whether or not true, the conclusion can be drawn that the person is a smoker or may be obese and that he or she may have health issues (such as lung or heart problems) because of this. The mere fact that a person uses a health app already can say a lot about their health, and even more so when the data is combined with other health information about a person. For example, an employer or insurer buying health data and combining it with the information already on record not only violates privacy but can also discriminate against their employee or the insured. This could lead to increases in insurance fees, rejection of insurance and perhaps even in unemployment. Data generated by modern technologies which can conclude something about a person's health in the broadest sense can therefore generally be seen as health data.

Health data has had a long history of being seen as a special category of data, also referred to as sensitive data, that requires additional protection. As such, Article 9 of the GDPR prohibits the processing of health data unless there is a legal basis to do so. If there is no legal basis for processing, the processing is considered to be unlawful. According to the GDPR, explicit consent given by the data subject is the legal basis for processing health data by modern technologies [20, 21]. The GDPR thus allows processing of personal health data by companies when a data subject explicitly consents. Consent of the data subject within the meaning of the GDPR means a clear affirmative act establishing at least the freely given, informed indication that the data subject agrees to the processing of his or her personal data [22]. Consent can also be given by

electronic means, for example by ticking a box when visiting a website, choosing certain technical settings or any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing. Pre-ticked boxes or inactivity by the data subject do not constitute consent [23]. The request for consent has to be clear, concise, not unnecessarily disruptive and needs to be presented in a clearly distinguishable form, meaning that it may not be buried within the fine print of a privacy policy or contract [24].

While at first sight it looks as if the GDPR offers sufficient protection against the processing of health data, the practical reality is quite different. Previous research has shown that companies offering health apps are by no means transparent about their processing activities and whom they share the data with [25]. While data subjects to some degree consent to data processing, some health apps do not even recognize the fact that they process health data, resulting in a lack of legal basis. As a result of this, risks of violation of rights and freedoms remain, as well as physical and practical challenges related to the use of modern technologies to process health data, such as jurisdiction and exercise of rights.

3. BEHIND THE SCENES OF MODERN TECHNOLOGIES

Processing personal data according to the GDPR includes 'collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction' of data [26]. This very broad definition means that basically any action performed on personal data is processing. The one word that is missing from the definition is *transfer* of data. What is however mentioned by the definition in Article 4 (2) GDPR is that processing also includes *disclosing the data by transmission* and *dissemination or otherwise making it available*. While it is interesting that transfer is not included in the definition for processing, disclosing and making data available can be seen as transfer of data.

Transfer has an important role in the GDPR. While the free flow of information has always been promoted by data protection legal frameworks, the major concern was that data protection legislation could be circumvented by moving processing operations to countries with no or less strict data protection laws [27]. European data protection legal frameworks have therefore always been cautious about transferring data to third countries who are not part of the legal regime. In order to prevent data from being transferred to 'data havens', the *principle of equivalent protection* was introduced, meaning that there should be no restrictions on transborder data flows to states with legal regimes which ensure data protection equivalent to data protection offered by the GDPR. Chapter V of the GDPR is dedicated to *transfers of personal data to third countries or international organisations*. Modern technologies process data electronically, making it easy to transfer data across the globe. The data can be sent from one actor to another or made accessible to more than one actor in a blink of an eye. Modern technologies thus impact the way that personal health data can be collected.

These modern technologies, such as mobile applications and wearables process large amounts of personal (health) data. The technologies make it possible to continuously monitor the user. Most people carry their mobile phone with them during the day and wearables made tracking even easier. A smart watch or smart glasses for example allow users to track their health and fitness with objects which are easy to carry. While making life and health easy for users, large amounts of health data become available to commercial companies who are by no means under any obligation of professional secrecy and what happens behind the scenes of these technologies is unknown to many. When unravelling what happens, behind the scenes, to the data we stumbled upon 2 major ways that the technologies function that are relevant for this article. Many health apps and wearables by default:

1. collect data via an app and store it on the device itself until the user actively choses to send the data to a cloud or server;
2. collect data via an app and store it on a (cloud) server. In this case the data exists outside of the app and is accessible to the developer, i.e. the device is used as a tool to collect data, the data can be seen separately from the app considering that it exists even if the app is deleted.

If we picture a user in the first situation and we take the example of an app that counts how many steps someone takes during the day, the app counts the steps and stores the data on the device itself by default. The data is stored on the device for as long as the user does not delete the data or chooses to store the data somewhere else, for example when the storage space of the device is full. In other words, the collected data remain on the user's device until the user actively decides to store the data elsewhere, outside of the app or wearable.

More importantly for this research is however the second situation, where data is collected by an app or wearable which does not intend to store it on the device. Instead, by default, the data is sent to and stored on the (cloud) server of the app company. Sending the data requires an active connection between the device and the (cloud) server. If this connection is unavailable, the data is most likely stored on the device until the connection is available.

There is a significant legal difference between the two situations. In the first situation the app is closely related to the data and therefore to the user, it is merely a means to an end. In the second situation, the purpose of the app or wearable is mainly to generate data. The device is not used for storage or not meant to be used for storage. As soon as an active connection is available, the data is sent to the

designated (cloud) server. In this regard, we can make an analogy with streaming data. The user might have the app on their mobile phone or wearable, but the data exists separately, outside this app. For example, when watching a YouTube video, the app is solely used to stream the data available on the YouTube server. While health apps and wearables are more of a two-way-street considering that they can also generate data, the basic concept and comparison to YouTube streaming is the same.

Processing health data in a way where data is collected by an app or wearable and sent to a (cloud) server for (further) processing still leaves the question whether sending the data can be seen as a transfer within the meaning of the GDPR and is as such protected or whether the device functions merely as a tool for the companies to collect data where sending the data can be seen as a mere transit of data [28]. The concept of 'transfer' will therefore be discussed in the next paragraph.

4. THE NOTION OF TRANSFER

The GDPR aims at offering a similar level of data protection, regardless of where in the world data of data subjects who are in the EU is being processed. Therefore, Chapter V of the GDPR includes provisions on transfers of personal data to third countries. This section provides rules in order to ensure data protection equivalent to the GDPR, meaning that data may only be transferred to third countries outside the EU if the conditions of the GDPR are met. In short, this means that there needs to be: 1) an adequacy decision (such as the EU-U.S. Privacy Shield) or 2) appropriate safeguards or 3) that the data subject has given explicit consent for data processing in the third country. With emerging modern technologies, where data may be processed anywhere in the world, it is of the utmost importance to protect the data, in particular health data. In order to establish whether sending data, from the app or wearable onto the (cloud) server of a company for the purpose of being processed by that company, can be seen as a transfer within the meaning of the GDPR, it is important to establish what transfer exactly is in order to determine whether or not it falls under Chapter V GDPR and consequently whether or not health data in this regard is sufficiently protected. In literature transfer is described as to *occur as a part of networked series of processes made to deliver a business result [29]*.

The GDPR is, however, unclear about what transfer is and does not provide a definition. What is clear is that it is a process where data moves between different actors. According to the European Data Protection Supervisor (EDPS) in its position paper on transfer to third countries and international organizations by EU institutions and bodies, the lack of a definition leads to the assumption that the term needs to be used in its natural meaning. As such transfer means that data 'moves' between different users. However, as the EDPS also concludes, this is not always straight forward. According to the Court of Justice of the European Union (CJEU) in the Lindqvist case, it is necessary to take account of both the technical nature of the operations carried out and of the purpose and structure of the provisions on transfer in EU legislation [30]. Taking into account the technical nature of processing operations, transfer, as such entails, among other things, the *automatically or intentionally sending or accessing of information*. Unfortunately, there is not a lot of case law in this regard to help further clarify the matter. If one of the factors determining what transfer is includes the technical nature by which it takes place, the question that arises is what technical circumstances can facilitate transfer. Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data [31] provides some insight in this regard.

Convention 108 includes a chapter on transborder data flows and determines that the provisions apply to the *transfer* across national borders *by whatever medium [32]*. It is aimed at the free flow of information, regardless of frontiers, taking into account the wide variety of factors determining the way in which data is transferred. These factors include: the mode of representation of the data, their storage medium, way of transport, interface, the circuit followed and the relations between the sender and recipient [33]. According to the explanatory memorandum the *way of transport* includes physical transport, mail, and circuit-switched or packet-switched telecommunications links. *The interface*, i.e. the point where two systems interact, can be, among other things, computer to terminal, computer to computer, and manual to computer. *The circuit followed* can be direct from the country of origin to the country of destination or via one or more countries of transit [34]. The explanatory report to the Modernized Convention provides some more clarity in determining that transborder data transfers occur when personal data is disclosed or made available to a *recipient* subject to the jurisdiction of another state or international organization. According to Article 2 (e) of the Convention a recipient is '*a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available*. The GDPR definition of recipient is almost the same, determining that *recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not' [35]*. The recipient thus receives the data or is given access to the data and can be a controller or a processor [36].

When it comes to moving data, there are two main ways to technically do this, namely by *exchanging* or *sharing* data. According to Doan et al. *data exchange* is the process of taking data that is structured within the source database system and transforming it into data structured under a target database system [37]. In other words, the data is transformed so that it becomes compatible with other systems which receive an accurate representation of the source data. Exchange thus allows data to be shared between systems and programs. The introductory report for updating Recommendation No. R (97) 5 defines exchange as *the communication of information to (a) clearly identified recipient(s) by a known transmitter (such as*

secured e-mailing) [38]. When health data is exchanged, the data is sent from A to B using a transmitter. This can be an e-mail or other way of sending the data so that it can be read and used by B. Figure 1 below shows this process. In this case, A is the original controller of the health data and B becomes the new controller of the data and will build on the received data for their own purpose.

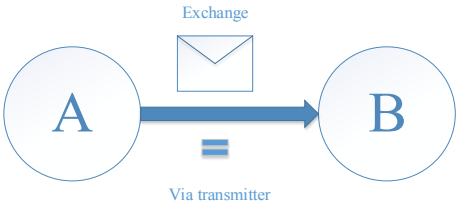

Figure 1 – Exchange

Data sharing on the other hand is making data available to others through a variety of mechanisms [39]. According to the introductory report for updating Recommendation No. R (97) 5 sharing is *making information accessible to third parties not necessarily identified at the time of the pooling and according to a principle of permissions (such as shared electronic medical records) [40]*. Figure 2 below shows how, in a sharing system, various recipients (A – H) can access the data for the purpose processing it. A – H are not necessarily known at the time of pooling and need permission to access the data.

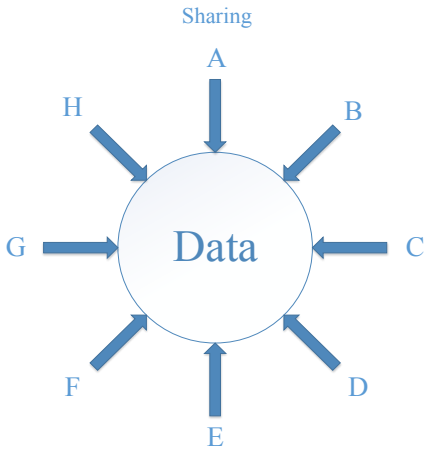

Figure 2 – Sharing

Both sharing and exchange of data are thus commanded by interoperable data processing systems and by common reference frameworks [40]. This allows health data to be moved or to be made accessible to a variety of actors. Considering that transfer can be automatically or intentionally sending information or making it accessible to a recipient by whatever medium, transfer can be both exchange and sharing of data. While exchange and sharing describe different ways of moving health data, both ways are a transfer of data. Taking the above-mentioned into account, the following conclusions can be drawn about transfer:

- Transfer does not have a legal meaning.
- Transfer has a natural meaning, i.e. data moves between users.
- Transfer may be the exchange or sharing of data.
- Data movement takes place by whatever medium.
- Data is disclosed or made available to a recipient.

5. TRANSFER OR TRANSIT?

When applying the notion of transfer to our case, where health data is being processed by commercial companies by modern technologies and the data is sent from the user's device to the (cloud) server of the company, sending this data can be seen as movement, even as an exchange of data between the user and the company, which takes place automatically and electronically. However, the GDPR applies to the processing of personal data of data subjects who are in the EU by a controller or processor regardless of whether the controller or processor is established in the EU. The actors in this case are the data subject who is the user of the app or wearable and the controller which is the company processing the data by modern technologies. The data subject does not determine the purpose and means and cannot be the controller of the data. Taking into account that the data exists separately from, i.e. outside the app, it is not the data subject who (actively) transfers the data to the company. The company as the controller cannot be both the controller of the data and the recipient to whom the data is disclosed. While sending the data may be seen as movement of data which can be a transfer of data, it remains difficult to classify processing by modern technologies as transfer of data. Consequentially, two questions arise. The first question is: if it is not a transfer of data, what is it then?

The Article 29 Working Party in its 2010 opinion on applicable law [41] mentions transit through EU territory, for example by way of telecommunication networks or postal services which ensure that communications are reached in third countries. While the context is slightly different, in our view the analogy can be made with modern technologies. When data is processed by modern technologies, the processing may take place anywhere in the world. For the data to reach the (cloud) server, a transit from the device to the server is necessary. Like an envelope containing data sent by post to a company outside the EU where it will undergo processing, a transit is required for the data to reach its destination. The data is simply being passed on and not being processed along the way [42]. In this case sending the data from the user's device to the (cloud) server of a company where it will undergo processing can be seen as a mere transit of data and cannot be classified as transfer within the meaning of the GDPR. The device on which the app is installed is a mere tool for companies to collect the data, which does not exist on the device, but on a (cloud) server owned by the company, which can be located anywhere in the world.

The second question is: if it is not transfer and the GDPR rules on transfer do not apply, is processing of health data by modern technologies sufficiently protected? Previous research [43] has shown that there is a gap between the GDPR and practical reality. There is a general lack of transparency from commercial companies about their processing activities, their purposes for processing, the quantity of health data processed, the location of storage and recipients the data is shared with. In particular, the sharing of data is of a great concern as the data is collected and shared with actors who are by no means under any obligation of professional secrecy and who sell the data to the highest bidder which may lead to various forms of discrimination, violation of fundamental rights and difficulties with exercising rights in case of infringements. This is even more concerning considering that people generally do not inform themselves before giving away their data and/ or choose convenience over privacy. It is the responsibility of companies to protect their users' privacy; however, unfortunately they often fail to do so. Consent as a legal basis for processing health data by modern technologies is therefore not enough. As a result of this, the complexity of the GDPR legal framework does not offer sufficient protection for processing of health data by modern technologies.

6. CONCLUSION

The multitude of modern technologies that are available today process large amounts of health data. When processing data, controllers and processors need to abide by the GDPR, which requires that there needs to be a legal basis for processing. Commercial companies therefore need to request the users of their modern technologies for consent before being allowed to process health data. On many occasions, these companies collect data via an app and store it on a (cloud) server where it is being processed. The device is used as a tool to collect data and the data can be seen separately from the app considering that it exists outside of the app (even if the app is deleted) where it is accessible to the company. Taking into consideration that the data exists outside the app and that the data subject cannot be the controller of his or her own data, the transfer regime of the GDPR does not apply when the data is being sent from the device to the (cloud) server. This process is a mere transit of data.

Considering that the GDPR transfer regime does not apply, the question is whether consent as a legal basis is enough. While the GDPR applies to the processing of the data of data subjects who are in the EU, regardless of where the controller or processor is established, the reality remains that it is more difficult to track data processed by modern technologies, i.e. where it is stored and with whom is it shared, which may result in discrimination and violation of rights. There is a general lack in transparency from companies as regards to their processing operations. Furthermore, informing people via privacy policies of modern technologies does not offer sufficient protection considering that most people do not actually read them [45]. And even if they were to read them, they might not understand the meaning or the risks involved. As such, people do not know what they are consenting to. Therefore, combining the fact that commercial companies are generally not transparent enough about their processing activities with the fact that users generally do not know what they are consenting to, results in a weak legal basis. As a consequence, violations take place more frequently than we would wish.

As such, the complexity of the GDPR legal framework does not offer sufficient protection against data processing by modern technologies and commercial companies are not taking sufficient responsibility when processing health data. Perhaps the solution lies in prohibiting the use of health data in certain situations as suggested by Frank Pasquale [44]. A stricter approach, i.e. prohibiting the use of health data in certain situations, would at least be an incentive for companies not to violate the privacy of a person's most intimate sphere. This approach will require further research on how to limit processing health data by modern technologies. The situations where it might be limited or prohibited would have to be defined. It is, however, our opinion that we need another way of looking at health data processed by modern technologies that would be beneficial to all parties and still protects rights and freedoms.

REFERENCES

[1] Council of Europe, Explanatory memorandum to Recommendation No. R (81) 1 of the Committee of Ministers to member states on regulations for automated medical data banks [1981], para. 6.

[2] B. Millington, 'Smartphone Apps and the Mobile Privatization of Health and Fitness', *Critical Studies in Media Communication,* v31 n5, December 2014, p. 479-493.

[3] M. L. Flear et al., European Law and New Health Technologies, Oxford: University Press, 2013, p. 1.

[4] Editorial, *An app a day is only a framework away*, Elsevier, The Lancet Digital Health, Volume 1, Issue 2, June 2019, Page e45, available at https://www.sciencedirect.com/science/article/pii/S2589750019300317.

[5] See for example: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases and https://decorrespondent.nl/8480/this-fitness-app-lets-anyone-find-names-and-addresses-for-thousands-of-soldiers-and-secret-agents/260810880-cc840165.

[6] See for example: https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-

public-than-you-think/?noredirect=on&utm_term=.7f91beb5e812.

[7] See for example: https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636?mod=e2tw and https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens>.

[8] See: https://theoutline.com/post/7039/there-is-a-reason-apps-make-it-so-fun-to-track-your-health.

[9] T. Mulder, M. Tudorica, Privacy policies, cross-border health data and the GDPR, *Information & Communications Technology Law* (2019) 28,3.

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[11] See for example: The concept of 'transfer' of data under European data protection law – in the context of transborder data flows, Faculty of Law – University of Oslo, 01-12-2015, available at: https://www.duo.uio.no/bitstream/handle/10852/49722/8026_The-concept-of-transfer-of-data-under-European-data-protection-law---In-the-context-of-transborder-data-flows.pdf?sequence=1&isAllowed=y.

[12] Articles 2 and 3 GDPR.

[13] N. Dasko, 'The General Data Protection Regulation (GDPR) – A Revolution Coming of European Data Protection Laws in 2018. What's New for Ordinary Citizens?', *Comparative Law Review*, p. 128, available at: http:h//tdtpx:./d/odix.o.drgo/i.1o0rg.g1/21707.152/7C77L7R5./2C0L1R7.2.00156.

[14] T. Mulder, M. Tudorica, Privacy policies, cross-border health data and the GDPR, *Information & Communications Technology Law* (2019) 28,3.

[15] Article 4 (15) GDRP.

[16] The EDPB is the independent European advisory body on data protection.

[17] Article 29 Data Protection Working Party, Letter to Mr. Timmens and Annex – health data in apps and devices, 2015, available at: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf and https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

[18] Article 29 Working Party (A29WP), Annex by letter – health data in apps and device, 2015 p. 5.

[19] According to Article 5 (1, a) GDPR.

[20] Article 9 (2,a) GDPR.

[21] Article 6 (a) GDPR.

[22] Article 4 (11) GDPR.

[23] Recital 32 GDPR. See also L. Golba, 'Consent for Personal Data Processing in Digital Environment According to GDPR', *Annuals of the Administration and Law*, no. 17 (2), p. 253-265.

[24] Article 7 (1) GDPR.

[25] See for example: https://www.theguardian.com/technology/appsblog/2013/sep/03/fitness-health-apps-sharing-data-insurance; T. Mulder, 'Health Apps, their Privacy Policies and the GDPR', European Journal of Law and Technology, (10) 1 (2019).

[26] Article 4 (2) GDPR.

[27] Council of Europe, "Explanatory report to the Convention for the protection of individuals with regard to automatic processing of personal data" (ETS No 108), para. 9.

[28] See for example: The concept of 'transfer' of data under European data protection law – in the context of transborder data flows, Faculty of Law – University of Oslo, 01-12-2015, available at: https://www.duo.uio.no/bitstream/handle/10852/49722/8026_The-concept-of-transfer-of-data-under-European-data-protection-law---In-the-context-of-transborder-data-flows.pdf?sequence=1&isAllowed=y.

[29] P.M. Schwartz, 'Managing Global Data Privacy' (2009) Privacy Projects, p. 4.

[30] Case C-101/01 *Criminal proceedings against Bodil Lindqvist* [2015] ECLI:EU:C:2003:596. In the Lindqvist case one of the question was whether there was 'transfer of data' when personal data is loaded onto an Internet page which is stored on an Internet site on which the page can be consulted, thereby making the data accessible to anyone who connects to the Internet, including people in a third country. As regards the technical nature of the operations, the Court concluded that the Internet pages in question did not contain the technical means to send information automatically to people who did not intentionally seek access to those pages. Internet users would have to connect to the Internet and personally carry out the necessary actions to consult those pages. As such, the data was not directly transferred between the person uploading the information to the website and persons entering the website. The CJEU refers to the provisions on transfer in Chapter IV of Directive 95/46/EC, which has been replaced by Chapter V of the GDPR.

[31] Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108.

[32] Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108, Article 12.

[33] Council of Europe, "Explanatory report to the Convention for the protection of individuals with regard to automatic processing of personal data" (ETS No 108), para. 62, 63.

[34] Council of Europe, "Explanatory report to the Convention for the protection of individuals with regard to automatic processing of personal data" (ETS No 108), para. 63.

[35] Article 4 (9) GDPR.

[36] Council of Europe, "Explanatory report to the Protocol amending the Convention for the protection of individuals with regard to automatic processing of personal data" (ETS No 223), para. 23.

[37] Doan, A., Halevy, A, Ives, Z., *Principles of data integration*, Elsevier: Morgan Kaufman, 2012, p. 276.

[38] J. Bossi Malafosse et. al., Introductory report for updating recommendation R (97) 5 of the Council of Europe on the protection of medical data, 2015, T-PD(2015)07, available at: https://rm.coe.int/introductory-report-for-updating-recommendation-r-97-5-of-the-council-/168073510c.

[39] C. Cava et al., Bioinformatics clouds for high-throughput technologies, in: *Handbook of research on cloud infrastructures for big data analytics*, 2014, p. 489 – 507.

[40] J. Bossi Malafosse et. al., Introductory report for updating recommendation R (97) 5 of the Council of Europe on the protection of medical data, 2015, T-PD (2015)07, available at https://rm.coe.int/introductory-report-for-updating-recommendation-r-97-5-of-the-council-/168073510c.

[41] Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, WP179, p. 23, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf.

[42] The concept of 'transfer' of data under European data protection law – in the context of transborder data flows, Faculty of Law – University of Oslo, 01-12-2015, available at: https://www.duo.uio.no/bitstream/handle/10852/49722/8026_The-concept-of-transfer-of-data-under-European-data-protection-law---In-the-context-of-transborder-data-flows.pdf?sequence=1&isAllowed=y.

[43] T. Mulder, M. Tudorica, Privacy policies, cross-border health data and the GDPR, *Information & Communications Technology Law* (2019) 28,3.

[44] F. Pasquale, 'Redescribing Health Privacy: the Importance of Information Policy' (2014) 103 HJHLP 127.

[45] See for example: A M McDonald and L F Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 A Journal of Law and Policy for the Information Society 543; F Schaub and os, 'Designing Effective Privacy Notices and Controls' (2017) 99 IEEE Internet Computing 70.